

# National Cyber Alert System

[Archive](#)

## Cyber Security Bulletin SB09-327

### Vulnerability Summary for the Week of November 16, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities			
Primary Vendor -- Product	Description	Published	CVSS Score
2wire -- 1700hg 2wire -- 1701hg 2wire -- 1800hw 2wire -- 2071 2wire -- 2700hg 2wire -- 2701hg-t	The management interface on the 2wire Gateway 1700HG, 1701HG, 1800HW, 2071, 2700HG, and 2701HG-T with software before 5.29.52 allows remote attackers to cause a denial of service (reboot) via a %od%oa sequence in the page parameter to the xslt program on TCP port 50001, a related issue to CVE-2006-4523.	2009-11-17	7.8
arcadetradescrit -- arcade_trade_script	Arcade Trade Script 1.0 allows remote attackers to bypass authentication and gain administrative access by setting the adminLoggedIn cookie to true.	2009-11-18	7.5
ed_charkow -- supercharged_linking	SQL injection vulnerability in browse.php in Ed Charkow SuperCharged Linking allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-11-18	7.5
faslo -- faslo_player	Stack-based buffer overflow in Faslo Player 7.0 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long string in a .m3u playlist file.	2009-11-18	9.3
gimp -- gimp	Integer overflow in the read_channel_data function in plugins/file-psd/psd-load.c in GIMP 2.6.7 might allow remote attackers to execute arbitrary code via a crafted PSD file that triggers a heap-based buffer overflow.	2009-11-18	9.3
hp -- discovery&dependency_mapping_inventory	Unspecified vulnerability in HP Discovery & Dependency Mapping Inventory (DDMI) 2.5x, 7.5x, and 7.60 on Windows allows remote authenticated users to execute arbitrary code via	2009-11-17	9.0

	unknown vectors.		
invisionpower -- invision_power_board	Multiple SQL injection vulnerabilities in Invision Power Board (IPB or IP.Board) 3.0.0, 3.0.1, and 3.0.2 allow remote attackers to execute arbitrary SQL commands via the (1) search_term parameter to admin/applications/core/modules_public/search/search.php and (2) aid parameter to admin/applications/core/modules_public/global/lostpass.php. NOTE: on 20090818, the vendor patched 3.0.2 without changing the version number.	2009-11-18	7.5
itechscripts -- itechbids	Multiple SQL injection vulnerabilities in iTechBids 8.0 allow remote attackers to execute arbitrary SQL commands via the (1) user_id parameter to feedback.php, (2) cate_id parameter to category.php, (3) id parameter to news.php, and (4) productid parameter to itechd.php. NOTE: the sellers_othersitem.php, classifieds.php, and shop.php vectors are already covered by CVE-2008-3238.	2009-11-18	7.5
jos_de_ruijter -- superseriousstats	SQL injection vulnerability in user.php in Super Serious Stats (aka superseriousstats) before 1.1.2p1 allows remote attackers to execute arbitrary SQL commands via the uid parameter, related to an "incorrect regexp." NOTE: some of these details are obtained from third party information.	2009-11-17	7.5
jtips -- jtips	SQL injection vulnerability in the jTips (com_jtips) component 1.0.7 and 1.0.9 for Joomla! allows remote attackers to execute arbitrary SQL commands via the season parameter in a ladder action to index.php.	2009-11-18	7.5
linux -- kernel linux -- kernel	Buffer overflow in the kvm_vcpu_ioctl_x86_setup_mce function in arch/x86/kvm/x86.c in the KVM subsystem in the Linux kernel before 2.6.32-rc7 allows local users to cause a denial of service (memory corruption) or possibly gain privileges via a KVM_X86_SETUP_MCE IOCTL request that specifies a large number of Machine Check Exception (MCE) banks.	2009-11-19	7.2
linux -- kernel linux -- kernel	The collect_rx_frame function in drivers/isdn/hisax/hfc_usb.c in the Linux kernel before 2.6.32-rc7 allows attackers to have an unspecified impact via a crafted HDLC packet that arrives over ISDN and triggers a buffer under-read.	2009-11-19	7.2
linux -- kernel	Array index error in the gdth_read_event function in drivers/scsi/gdth.c in the Linux kernel before 2.6.32-rc8 allows local users to cause a denial of service or possibly gain privileges via a negative event index in an IOCTL request.	2009-11-20	7.2
maniacomputer -- new5starrating	SQL injection vulnerability in rating.php in New 5 star Rating 1.0 allows remote attackers to execute arbitrary SQL commands via the det parameter.	2009-11-18	7.5
microsoft -- windows_7 microsoft -- windows_server_2008	The kernel in Microsoft Windows Server 2008 R2 and Windows 7 allows remote SMB servers to cause a denial of service (infinite loop and system hang) via a (1) SMBv1 or (2) SMBv2 response packet that contains a NetBIOS header with an incorrect length value, which triggers an assertion failure in the KeAccumulateTicks function.	2009-11-13	7.1
ninjaforge -- ninjamonials	SQL injection vulnerability in the NinjaMonials (com_ninjacentral) component 1.1.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the testimID parameter in a display action to index.php.	2009-11-18	7.5
qproje -- siirler_bileseni	SQL injection vulnerability in the Q-Proje Siirler Bileseni (com_siirler) component 1.2 RC for Joomla! allows remote attackers to execute arbitrary SQL commands via the sid parameter in an sdetay action to index.php.	2009-11-18	7.5

rhinosoft -- serv-u	Stack-based buffer overflow in the TEA decoding algorithm in RhinoSoft Serv-U FTP server before 9.1.0.0 allows remote attackers to execute arbitrary code via a long hexadecimal string.	2009-11-20	<a href="#">9.0</a>
tandberg -- tandberg_mxp_endpoints	Buffer overflow in the FTP service on the Tandberg MXP F7.0 allows remote attackers to cause a denial of service (process crash or device reboot) or possibly execute arbitrary code via a long USER command, as demonstrated by a command ending with many space characters.	2009-11-16	<a href="#">9.3</a>
turnkeyarcade -- turnkey_arcade_script	SQL injection vulnerability in index.php in Turnkey Arcade Script allows remote attackers to execute arbitrary SQL commands via the id parameter in a browse action, a different vector than CVE-2008-5629.	2009-11-18	<a href="#">7.5</a>
vivaprograms -- infinity_script	cp/profile.php in VivaPrograms Infinity 2.0.5 and earlier does not require administrative authentication for the donewauthor action, which allows remote attackers to create administrative accounts via the name, password, and conf_password parameters.	2009-11-16	<a href="#">7.5</a>
xoops --xoops	Multiple unspecified vulnerabilities in XOOPS before 2.4.0 Final have unknown impact and attack vectors.	2009-11-17	<a href="#">7.5</a>

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- safari	WebKit, as used in Apple Safari before 4.0.4 and Google Chrome before 3.0.195.33, includes certain custom HTTP headers in the OPTIONS request during cross-origin operations with preflight, which makes it easier for remote attackers to conduct cross-site request forgery (CSRF) attacks via a crafted web page.	2009-11-13	<a href="#">6.8</a>	<a href="#">CVE-2009-2816 CONFIRM APPLE</a>
apple -- cups	Use-after-free vulnerability in the abstract file-descriptor handling interface in the cupsdDoSelect function in scheduler/select.c in the scheduler in cupsd in CUPS 1.3.7 and 1.3.10 allows remote attackers to cause a denial of service (daemon crash or hang) via a client disconnection during listing of a large number of print jobs, related to improperly maintaining a reference count. NOTE: some of these details are obtained from third party information.	2009-11-19	<a href="#">5.0</a>	<a href="#">CVE-2009-3553 MISC MISC MISC MISC MISC</a>
bestpractical -- rt	Cross-site scripting (XSS) vulnerability in Best Practical Solutions RT 3.6.x before 3.6.9, 3.8.x before 3.8.5, and other 3.4.6 through 3.8.4 versions allows remote attackers to inject arbitrary web script or HTML via certain Custom Fields.	2009-11-17	<a href="#">4.3</a>	<a href="#">CVE-2009-3892 MLIST MLIST</a>
bract -- suntrack	Multiple cross-site scripting (XSS) vulnerabilities in Bractus SunTrack allow remote attackers to inject arbitrary web script or HTML via the (1) title parameter to newprofile.html; the (2) firstname, (3) lastname, and (4) company parameters to signup/signup.html; and the (5) firstname, (6) lastname, and (7) address[o].street1 parameters to contact.html.	2009-11-16	<a href="#">4.3</a>	<a href="#">CVE-2009-3950 BUGTRAQ</a>
	Unspecified vulnerability in Citrix Online Plug-in for			

citrix -- online_plug-in_for_mac citrix -- online_plug-in_for_windows citrix -- receiver_for_iphone	Windows 11.0.x before 11.0.150 and 11.x before 11.2, Online Plug-in for Mac before 11.0, Receiver for iPhone before 1.0.3, and ICA Java, Mac, UNIX, and Windows Clients for XenApp and XenDesktop allows remote attackers to impersonate the SSL/TLS server and bypass authentication via a crafted certificate, a different vulnerability than CVE-2009-3555.	2009-11-13	5.8	CVE-2009-3936 VUPEN CONFIRM
cowonamerica -- cowon_media_center-jetaudio	JetAudio 7.5.3 COWON Media Center allows remote attackers to cause a denial of service (memory consumption and application crash) via a long string at the end of a .wav file.	2009-11-16	4.3	CVE-2009-3948 XF MILWORM
hp -- openview_network_node_manager	The embedded database engine service (aka ovdbrun.exe) in HP OpenView Network Node Manager (OV NNM) 7.51 and 7.53 allows remote attackers to cause a denial of service (daemon crash) via an invalid Error Code field in a packet.	2009-11-18	5.0	CVE-2009-3840 BID HP HP
hp -- openview_network_node_manager	Multiple buffer overflows in a certain ActiveX control in ActiveDom.ocx in HP OpenView Network Node Manager (OV NNM) 7.53 might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via a long string argument to the (1) DisplayName, (2) AddGroup, (3) InstallComponent, or (4) Subscribe method. NOTE: this issue is not a vulnerability in many environments, because the control is not marked as safe for scripting and would not execute with default Internet Explorer settings.	2009-11-18	5.0	CVE-2009-3977 MISC
ibm -- websphere_application_server	Cross-site request forgery (CSRF) vulnerability in the administrative console in the Security component in IBM WebSphere Application Server (WAS) 6.0.2 before 6.0.2.39, 6.1 before 6.1.0.29, and 7.0 before 7.0.0.7 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2009-11-16	6.8	CVE-2009-2746 CONFIRM
joomla -- joomla!	Unspecified vulnerability in the Front-End Editor in the com_content component in Joomla! before 1.5.15 allows remote authenticated users, with Author privileges, to replace the articles of an arbitrary user via unknown vectors.	2009-11-16	5.5	CVE-2009-3945 XF SECUNIA OSVDB CONFIRM
joomla -- joomla!	Joomla! before 1.5.15 allows remote attackers to read an extension's XML file, and thereby obtain the extension's version number, via a direct request.	2009-11-16	5.0	CVE-2009-3946 XF OSVDB SECUNIA CONFIRM
linux -- kernel	The do_mmap_pgoff function in mm/nommu.c in the Linux kernel before 2.6.31.6, when the CPU lacks a memory management unit, allows local users to cause a denial of service (OOPS) via an application that attempts to allocate a large amount of memory.	2009-11-16	4.9	CVE-2009-3888 CONFIRM
linux -- kernel	The dbg_lvl file for the megaraid_sas driver in the Linux kernel before 2.6.27 has world-writable permissions, which allows local users to change the (1) behavior and (2) logging level of the driver by modifying this file.	2009-11-16	6.6	CVE-2009-3889 MISC MLIST MLIST CONFIRM CONFIRM
linux -- kernel	The poll_mode_io file for the megaraid_sas driver in the Linux kernel 2.6.31.6 and earlier has world-writable permissions, which allows local users to change the I/O mode of the driver by modifying this file.	2009-11-16	6.6	CVE-2009-3939 MISC MLIST

martin_lambers -- mpop	Martin Lambers mpop before 1.0.19, when OpenSSL is used, does not properly handle a '\o' character in a domain name in the (1) subject's Common Name or (2) Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-11-16	5.0	CVE-2009-3941 VUPEN CONFIRM
martin_lambers -- msmtpt	Martin Lambers msmtpt before 1.4.19, when OpenSSL is used, does not properly handle a '\o' character in a domain name in the (1) subject's Common Name or (2) Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-11-16	6.4	CVE-2009-3942 VUPEN SECUNIA CONFIRM
microsoft -- ie	Microsoft Internet Explorer 6 through 6.0.2900.2180 and 7 through 7.0.6000.16711 allows remote attackers to cause a denial of service (application hang) via a JavaScript loop that configures the home page by using the setHomePage method and a DHTML behavior property.	2009-11-16	5.0	CVE-2009-3943 BUGTRAQ BUGTRAQ MISC
moagallery -- moa	SQL injection vulnerability in index.php in Moa Gallery 1.1.0 and 1.2.0 allows remote attackers to execute arbitrary SQL commands via the gallery_id parameter in a gallery_view action.	2009-11-18	6.8	CVE-2009-3975 XF VUPEN MILWORM SECUNIA
mozilla -- firefox	The nsGIFDecoder2::GifWrite function in decoders/gif/nsGIFDecoder2.cpp in libpron in Mozilla Firefox before 3.5.5 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an animated GIF file with a large image size, a different vulnerability than CVE-2009-3373.	2009-11-18	4.3	CVE-2009-3978 CONFIRM MISC MISC
mozilla -- bugzilla	Template.pm in Bugzilla 3.3.2 through 3.4.3 and 3.5 through 3.5.1 allows remote attackers to discover the alias of a private bug by reading the (1) Depends On or (2) Blocks field of a related bug.	2009-11-20	5.0	CVE-2009-3386 CONFIRM VUPEN BID CONFIRM
phpdirsubmit -- php_dir_submit	SQL injection vulnerability in index.php in PHP Dir Submit (aka WebsiteSubmitter or Submitter Script) allows remote authenticated users to execute arbitrary SQL commands via the aid parameter in a showarticle action.	2009-11-18	6.5	CVE-2009-3970 XF VUPEN MILWORM
proftpd -- proftpd	Buffer overflow in Labtam ProFTP 2.9 allows remote FTP servers to cause a denial of service (application crash) or execute arbitrary code via a long 220 reply (aka connection greeting or welcome message).	2009-11-18	6.8	CVE-2009-3976 XF VUPEN BID MILWORM
rim -- blackberry_browser rim -- blackberry_8800	Research In Motion (RIM) BlackBerry Browser on the BlackBerry 8800 allows remote attackers to cause a denial of service (application hang) via a JavaScript loop that configures the home page by using the setHomePage method and a DHTML behavior property.	2009-11-16	5.0	CVE-2009-3944 BUGTRAQ
	Unrestricted file upload vulnerability in the wp_check_filetype function in wp-includes/functions.php in WordPress before 2.8.6, when a certain configuration of the mod_mime module in the Apache HTTP Server is enabled, allows	2009-11-17	6.0	CVE-2009-3890 MLIST

wordpress -- wordpress	remote authenticated users to execute arbitrary code by posting an attachment with a multiple-extension filename, and then accessing this attachment via a direct request to a wp-content/uploads/ pathname, as demonstrated by a .php.jpg filename.	2009-11-17	0.0	<a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
------------------------	--	------------	-----	---

[Back to top](#)**Low Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sun -- virtualbox sun -- xvm_virtualbox	Unspecified vulnerability in Guest Additions in Sun xVM VirtualBox 1.6.x and 2.0.x before 2.0.12, 2.1.x, and 2.2.x, and Sun VirtualBox before 3.0.10, allows guest OS users to cause a denial of service (memory consumption) on the guest OS via unknown vectors.	2009-11-16	<a href="#">2.1</a>	<a href="#">CVE-2009-3940</a> <a href="#">SUNALERT</a>
wordpress -- wordpress	Cross-site scripting (XSS) vulnerability in wp-admin/press-this.php in WordPress before 2.8.6 allows remote authenticated users to inject arbitrary web script or HTML via the s parameter (aka the selection variable).	2009-11-17	<a href="#">3.5</a>	<a href="#">CVE-2009-3891</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

[Back to top](#)**Last updated November 23, 2009**
 [Print This Document](#)